IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A data processing system for generating at least one first unique base key and one second unique base key, comprising a cryptographic device including at least one master group key, at least one first security token and one second security token including respectively a first unique identifier and a second unique identifier, and a communication component for exchanging data between said cryptographic device and said first and second tokens, wherein:

said cryptographic device includes a logic operator that combines said at least one master group key with said first unique identifier received from said first security token through said communication component, producing said at least one first unique base key, and that combines said at least one master group key with said second unique identifier received from said second security token through said communication component, producing said at least one second unique base key,

said at least one first security token includes a first data storage that stores said at least one first unique base key and a

first cryptographic section that uses said stored at least one first unique base key, and

said at least one second security token includes a second data storage that stores said at least one second unique base key and a second cryptographic section that uses said stored at least one second unique base key.

2. (Previously Presented) The system according to claim 1, wherein said logic operator includes an exclusive OR bit-wise operator.

3. (Previously Presented) The system according to claim 2, wherein said first and second unique identifiers and said master group key are used as operands by said exclusive OR bit-wise operator forming respectively said at least one first and second unique base keys.

4. (Previously Presented) The system according to claim 1 further including a message digest function section that digests said unique identifier before operation by said logic operator.

5. (Previously Presented) A method of generating at least one first unique base key and one second unique base key, comprising:

generating a master group key by a cryptographic device,

receiving a first unique identifier from a first security token by said cryptographic device,

performing a logic operation using said first unique identifier and said master group key as operands producing said at least one first unique base key,

operatively injecting said at least one first unique base key into said first security token,

receiving a second unique identifier from a second security token by said cryptographic device,

performing a logic operation using said second unique identifier and said master group key as operands producing said at least one second unique base key, and

operatively injecting said at least one second unique base key into said second security token.

6. (Original) The method according to claim 5, further comprising the steps of digesting said unique identifier using a message digest function.

7. (Original) The method according to claim 6, wherein said logic operation includes an exclusive OR bit-wise operation.

8. (Previously Presented) A system for performing symmetric keys based mutual authentications between at least two security tokens, comprising:

a first security token including a first unique identifier, a first unique base key which is a function of a master key and of said first unique identifier, a first cryptographic section, and a first memory storage section,

a second security token including a second unique identifier, a second unique base key which is a function of said master key and of said second unique identifier,

a second cryptographic section compatible with said first cryptographic section, and a second memory storage section, and

a communication section that exchanges data between said first and second security tokens, wherein:

said first security token comprises a first logic operator that processes said first unique base key and said second unique identifier received from said second security token, producing a first composite group key,

said second secure security token comprises a second logic operator that processes said second unique base key and said

first unique identifier received from said first security token, producing a second composite group key, and

said first and second composite group keys are equal.

9. (Previously Presented) The system according to claim 8 wherein said second unique identifier processed by said first logic operator is a message digest of said second unique identifier, said first security token comprising a first message digest function section that digests said second unique identifier received using said communications section from said second security token.

10. (Previously Presented) The system according to claim 9 wherein said first unique identifier processed by said second logic operator is a message digest of said first unique identifier, said second security token comprising a second message digest function section that digests said first unique identifier received using said communications section from said first security token.

11. (Previously Presented) The system according to claim 10 wherein said first logic operator comprises a first exclusive OR bit-wise operator, said message digest of said second unique

identifier and said first unique base key being used as operands by said first exclusive OR bit-wise operator, producing said first composite group key which is stored using said first memory storage section.

12. (Previously Presented) The system according to claim 11 wherein said second logic operator comprises a second exclusive OR bit-wise operator, said message digest of said first unique identifier and said second unique base key being used as operands by said second exclusive OR bit-wise operator, producing said second composite group key which is stored using said second memory storage section.

13. (Previously Presented) The system according to claim 12 wherein said first security token comprises first random number generating section that generates a first random number, said first random number being stored using said first memory storage section, said first cryptographic section encrypting said first random number with said first composite group key producing a first cryptogram.

14. (Previously Presented) The system according to claim 13 wherein said second security token comprises second random

number generating section that generates a second random number, said second random number being stored using said second memory storage section, said second cryptographic section encrypting said second random number with said second composite group key producing a second cryptogram.

15. (Previously Presented) The system according to claim 14 wherein said first cryptogram is sent to said second security token using said communications section and decrypted using said second composite group key and said second cryptographic section, producing a first random number result.

16. (Previously Presented) The system according to claim 15 wherein said second cryptogram is sent to said first security token using said communications section and decrypted using said first composite group key and said first cryptographic section, producing a second random number result.

17. (Previously Presented) The system according to claim 16 wherein said first random number result is sent to said first security token using said communications section, said first security token comprising a first comparing section that compares

said first random number result to said first random number retrieved using said first memory storage section.

18. (Previously Presented) The system according to claim 17 wherein said second random number result is sent using said communications section to said second security token, said second security token comprising second comparing section that compares said second random number result to said second random number retrieved using said second memory storage section.

19. (Original) The system according to claim 17 wherein a match between said first random number result and said first random number authenticates said second security token to said first security token.

20. (Original) The system according to claim 18 wherein a match between said second random number result and said second random number authenticates said first security token to said second security token.

21. (Previously Presented) The system according to claim 8 wherein said first cryptographic section and said second

cryptographic section includes at least one common symmetric cryptographic algorithm.

22. (Previously Presented) A method for performing mutual authentications between a first security token and a second security token, comprising:

sending a first unique identifier from a first security token to a second security token,

sending a second unique identifier from said second security token to said first security token,

digesting said second unique identifier by said first security token using a message digest function mutually installed in said first and said second security tokens producing a second digest result,

digesting said first unique identifier by said second security token using said message digest function producing a first digest result,

performing an exclusive OR bit-wise operation by said second security token using said first digest result and a second unique base key as operands, producing a second composite group key, wherein said second unique base key is a function of a master key and of said second unique identifier,

performing an exclusive OR bit-wise operation by said first security token using said second digest result and a first unique base key as operands, producing a first composite group key, wherein said first unique base key is a function of said master key and of said first unique identifier, and wherein said first and second composite group keys are equal,

generating a first random number by said first security token, storing a copy of said first random number and encrypting said first random number using said first composite group key and a mutually shared cryptographic algorithm, producing a first cryptogram,

generating a second random number by said second security token, storing a copy of said second random number and encrypting said second random number using said second composite group key and said mutually shared cryptographic algorithm, producing a second cryptogram,

sending said first cryptogram from said first security token to said second security token,

sending said second cryptogram from said second security token to said first security token,

receiving and decrypting said first cryptogram using said second composite group key and said mutually shared cryptographic

algorithm by said second security token producing a first random number result,

receiving and decrypting said second cryptogram using said first composite group key and said mutually shared cryptographic algorithm by said first security token producing a second random number result,

sending said first random number result from said second security token to said first security token,

sending said second random number result from said first security token to said second security token,

receiving said first random number result by said first security token, retrieving said copy of said first random number from memory and comparing said first random number result to said copy of said first random number,

receiving said second random number result by said second security token, retrieving said copy of said second random number from memory and comparing said second random number result to said copy of said second random number,

authenticating said second security token to said first security token if said first random number result matches said copy of said first random number, and

authenticating said first security token to said second security token if said second random number result matches said copy of said second random number.

23. (Original) The method according to claim 22, wherein said mutually shared cryptographic algorithm is a symmetric algorithm.

24. (Original) A program storage device readable by a machine, tangibly embodying a program of instructions executable by said machine to perform the method steps of claim 5 or 22.